RÉPUBLIQUE ET CANTON DE GENÈVE

POST TENEBRAS LUX

Genève, le 13 avril 2022

Le Conseil d'Etat

1562-2022

Confédération Suisse
Département fédéral des finances
Monsieur Ueli Maurer
Conseiller fédéral
Bundesgasse 3
3003 Berne

Concerne : obligation de signaler les cyberattaques contre des infrastructures critiques

Monsieur le Conseiller fédéral,

Notre Conseil a pris connaissance des propositions transmises par le Département fédéral des finances (DFF) le 12 janvier 2022, concernant la consultation relative à l'obligation de signaler les cyberattaques contre des infrastructures critiques et sur la modification de la loi sur la sécurité de l'information (LSI), qui ont retenu notre meilleure attention.

Après analyse, nous sommes favorables, avec quelques réserves, aux propositions d'amendements à la LSI présentées.

Nous relevons toutefois un manque de cohérence avec la récente loi fédérale sur la protection des données (nLPD). Alors que cette dernière propose des règles et mécanismes précis d'annonce, par exemple lors de violations de la protection des données, certaines propositions – qui sont annoncées comme inspirées de la nLPD – s'appuient sur des règles et mécanismes différents. La collaboration indispensable avec le préposé fédéral à la protection des données et à la transparence est aussi absente.

En outre, certains points nécessitent d'être améliorés. Par exemple, alors que la loi spécifie explicitement que les communes sont concernées, le projet de loi fait implicitement porter tout le poids des interactions et responsabilités avec celles-ci sur le canton.

Vous trouverez en annexe de la présente réponse l'ensemble de nos commentaires.

En vous remerciant de nous avoir consulté, nous vous prions de croire, Monsieur le Conseiller fédéral, à l'expression de notre haute considération.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :

Michèle Righetti

Le président :

Serge Dal Busco

Annexe mentionnée

Copie à : ncsc@gs-efd.admin.ch

REPUBLIQUE ET CANTON DE GENEVE
Département des infrastructures
Office cantonal des systèmes d'information et du numérique

NOTE D'ACCOMPAGNEMENT

De :	Christian Geffcken et Pascal Verniory
A :	Confédération Suisse, Département fédéral des finances
Date :	23 mars 2022
Objet :	Loi fédérale sur la sécurité de l'information au sein de la Confédération (Loi sur la sécurité de l'information, LSI) Annexe

Ci-après, vous trouverez les commentaires ou propositions de changements formulées par l'office cantonal des systèmes d'information et du numérique (OCSIN) du canton de Genève.

Article 5, lettres d à e :
Il manque une définition de "cyberrisque" à l'art 1,1, b

Article 73b alinéa 1
Le paragraphe n'est pas clair.

En effet, la première phrase mentionne que le NCSC fera une analyse.

La seconde phrase précise « *pour autant que la situation ne nécessite pas d'analyses ou clarifications supplémentaires* ».

Dès lors, est-ce que ces « suppléments » se rapportent au signalement ou à l'analyse initiale du NCSC ? Le rapport explicatif n'évoque pas cette restriction.

Article 73b alinéa 1
[...] **pour autant que la situation ne nécessite pas d'analyses ou clarifications supplémentaires**
Nous proposons de remplacer cette partie de phrase comme suite :
[...] pour autant qu'il ne soit pas nécessaire d'instruire d'enquête complémentaire.

Article 73b alinéa 2
"Le NCSC **peut"** [...]

Cela n'engendre donc pas d'obligation. Néanmoins, quels seront les critères, et qui les déterminera ?

Article 73b alinéa 2
[...] et aux organisations **intéressées** [...]

Cela signifie-t-il que celles-ci doivent explicitement s'annoncer ? Et si oui, est-ce pour chaque cas, ou pour tous les cas ?

Article 73b alinéa 2
Nous estimons que ce terme « intéressées » est trop vague et pas forcément adéquat. Nous proposons de le remplacer par « concernées ».

Article 73b alinéa 2
[...] **et que la personne concernée ait donné son accord.**

Si deux millions de personnes sont concernées, est-ce que cela signifie que les 2 millions de personnes doivent donner leur accord ? Plus concrètement, qui est la personne concernée ?

Article 73b alinéa 2
[...] **et que la personne concernée ait donné son accord.**

Les personnes concernées n'ont pas à donner leur accord pour les raisons suivantes :
- Seules les organisations concernées sont contactées (cf. modification proposée ci-dessus)
- La démarche vise à améliorer la sécurité, donc se fait en faveur des personnes concernées
- Il s'agit de savoir quelle information transmettre aux personnes concernées.

Ces activités n'ont pas à être couvertes par l'accord des personnes intéressées. Il s'agit d'activités « internes » et dans un cercle limité. Quant aux communications au grand public et de nature préventive, la transmission de données personnelles ne devrait pas être nécessaire.

Article 73b alinéa 3
Le NCSC informe immédiatement **le fabricant [...]**

Nous estimons que tant le concepteur que le diffuseur devraient être concernés par l'annonce effectuée par le NCSC. Ainsi, nous proposons de répondre à la volonté affichée par la Confédération d'agir sur le matériel et le logiciel, et proposons la variante suivante : "le fabricant et/ou l'éditeur".

Article 73c alinéa 3
[...] ne peuvent être utilisées dans une procédure pénale contre **cette personne** [...]

Qu'en est-il de l'entreprise ou de l'administration qui emploie ladite personne ?
Nous estimons que cette disposition devrait plutôt s'appuyer sur la protection assurée par la loi sur les lanceurs d'alerte.

Article 73c alinéa 4
[...] **informations qui révèlent des secrets pénalement protégés**

L'article 320 du code pénal concerne un périmètre d'informations beaucoup plus large. Pourquoi le limiter ici ?

Article 74 alinéa 2, lettre c
Qui prend en charge la communication au grand public ? Comment est-ce fait ?

Article 74 alinéa 3
[...] correction des vulnérabilités lorsqu'il existe un risque **imminent** [...]

Comment est déterminée l'imminence du risque ?

Nous estimons que l'imminence des risques couverts par le PL implique que le NCSC conseille et aide les exploitants d'infrastructures critiques de manière immédiate à survenance du risque encouru. Ainsi, dès l'instant où ce soutien est de toute manière conditionné à la non-existence d'une alternative fournie par le marché privé, le "risque" de voir le NCSC fournir une prestation indue est faible.

Article 74a
[...] afin que **celui-ci** [...]

Est-ce le NCSC ou l'exploitant ? S'il s'agit du NCSC, il conviendrait de le préciser par « ce dernier ».

Article 74a
[...] **avertir les victimes potentielles** [...]

Cette phrase est en contradiction avec la LPD, qui prévoit que cette communication relève d'une décision du PFPDT. Une collaboration du NCSC avec ce dernier doit être prévue, car le signalement au PFPDT double celui prévu au NCSC et entraîne un risque important d'incohérence.

A notre sens, il incombe en premier lieu au NCSC de répondre à l'urgence commandée par une situation critique. Il lui revient de déclarer – dans un second temps administratif – au préposé fédéral à la protection des données tout incident touchant à la sphère de la LPD. Pour éviter tout risque de doublon entre le PL et la LPD, il conviendrait peut-être de faire figurer l'obligation pour le NCSC de déclarer l'événement au PFPDT.

Article 74b lettre b
[...] aux autorités fédérales, cantonales ou **communales** [...]

Dans ce cas, la Confédération doit communiquer directement avec les communes (ou les associations de communes), et ne pas se contenter de laisser les cantons s'en charger. Les urgences de la sécurité s'accommodent mal d'une telle hiérarchie verticale.

Quand bien même il est bien compris que la liste des infrastructures critiques est une reprise des sous-secteurs critiques tels que définis dans la stratégie nationale pour la protection des infrastructures critiques, il nous semble que les éléments suivants peuvent faire l'objet d'un commentaire :

- Généralités : les lettres f) et s) semblent recouvrir l'ensemble des acteurs directement concernés par l'action à mener par la NCSC. De fait, les interlocuteurs "en première ligne" vis-à-vis des événements critiques dont dispose le PL en question sont les exploitants, fabricants, éditeurs et/ou de prestataires de services (internes ou externes) à l'endroit des infrastructures critiques. Par ailleurs, sauf à connaître que la liste des infrastructures critiques figurent plutôt dans l'ordonnance d'application (adaptation facilitée) et non dans la loi, nous suggèrerions de structurer l'article en deux sous-section : la première qui concernerait les acteurs compris dans les lettres f) et s) avec obligation de signalement en premier chef vu leur responsabilité d'ordre technique, et une seconde, avec les entités considérées comme infrastructures critiques, avec une obligation de signalement basée sur leur qualité de propriétaire des données.

- Lettre f) : les notions de "grand nombre d'utilisateurs" et de "grande importance pour l'économie" gagneraient à être mieux précisées dans l'ordonnance que l'intention annoncée dans le commentaire de l'article considéré.

Article 74b, lettre f. 3.
offrent **des services de sécurité et de confiance;**

Cette notion de « services de sécurité et de confiance » est-elle définie dans une autre loi, par exemple la Loi sur la signature électronique ? À défaut, dans l'ordonnance d'application prévue ?

Article 74b, lettre g
La référence à l'article de la LAMAL est erronée. Il s'agit de l'article 39, al.1 (au lieu de l'article 9).

Nous proposons de changer la formulation de cet article de la manière suivante :"aux hôpitaux figurant sur la liste hospitalière cantonale des hôpitaux conformément à l'article 39, al. 1 let.e. de la loi fédérale du 18 mars 1994 sur l'assurance maladie, et, par analogie, aux établissements mentionnés à l'art. 39 al. 3 LAMAL.

Article 74b, lettre s. 4
[...] **cryptage** [...]

Le terme correct en français est « chiffrement » (source : ANSSI). Le terme « cryptage » est réservé à l'encodage de la télévision, style Canal+

Article 74c
Le Conseil fédéral exempte [...]

Cet article est en contradiction avec la LPD si l'obligation de signalement est au NCSC. Les causes d'exception sont par ailleurs inadéquates car il ne s'agit pas de savoir s'il convient de signaler les risques aux personnes concernées, mais au NCSC et cela devrait être à lui de trier de telles informations.

Par ailleurs, il convient de rappeler que la communication d'un risque non critique pour une entité peut s'avérer très critique pour d'autres. D'autre part, la communication simultanée de plusieurs attaques « non critiques » pourrait permettre au NCSC d'en déduire le début d'attaques concertées de plus grande échelle.

Article 74c, lettre b
n'ont qu'un impact limité [...]

Le projet d'article 74b liste un grand nombre d'institutions qui sont considérées comme suffisamment importantes.

Cette lettre b est contradictoire avec le but du 74b.

Article 74d, alinéa 1, lettre a
[...] **une autre infrastructure critique;**

Cette appréciation échappe très souvent à l'entité intéressée. Il serait donc préférable qu'elle communique d'office – même de manière succincte – au NCSC sans en faire une condition de la communication.

Article 74d, alinéa 2
Le principe de cet alinéa est louable. Cependant, dans la pratique, bien des entreprises et institutions ne pourraient se permettre de perdre leurs données chiffrées par un rançongiciel.

En violant cet article, elles s'infligeraient une double peine.

Au niveau de la teneur du signalement d'une cyberattaque, il nous apparaît que les informations devraient également inclure le produit logiciel ainsi que l'identité du prestataire de services informatiques

Article 74e, alinéa 1
[...] son **déroulement** et ses conséquences [...].

Nous proposons de préciser la phrase comme suite :
[...] déroulement, notamment les informations temporelles, et ses conséquences [...].

Article 74e, alinéa 1
[...] **ainsi que les mesures que compte prendre** l'exploitant [...]

Nous proposons de remplacer cette partie de phrase par :
[...] ou que l'entité concernée a commencé à mettre en œuvre

Article 74e, alinéa 2
[...] **dès que celles-ci lui parviennent**

Nous proposons de compléter cette phrase par [...] ou qu'elles peuvent être obtenues.

Article 74f, alinéa 1
Le NCSC **met** à disposition [...].

Nous proposition d'ajouter [...] **gratuitement** à disposition [...].

Article 74f, alinéa 2
Ce système doit permettre **à l'exploitant d'une infrastructure** [...]

Si cela se passe par le système du NCSC, c'est ce dernier qui communique, à la suggestion de l'entité concernée.

Article 74f, alinéa 3
[...] l'autorité concernés **ont besoin** [...]

Nous proposons de préciser : [...] ont **légitimement** besoin [...].

Article 74g
L'exploitant de l'infrastructure critique **fournit au NCSC** [...].

Nous proposons : [...] fournit **dans les meilleurs délais** au NCSC [...].

Article 74i, alinéa 1
Est puni **d'une amende de 100 000 francs** [...].

Au niveau du montant de l'amende encourue en cas de non-signalement, il peut raisonnablement être estimé que le faible montant de l'amende maximale ne remplisse pas son rôle incitatif pour des entreprises réalisant un chiffre d'affaires conséquent, Partant, nous nous demandons dans quelle mesure il ne serait pas opportun d'envisager soit un montant nominal max. plus important, soit un montant rapporté au chiffre d'affaires."

Article 75, alinéa 1, lettre a
[...] **le traitement des données** n'est admissible [...]

Nous proposons de préciser : [...] le traitement **de ces** données [...].

Article 76
Dans cet article, considère-t-on que « les exploitants d'infrastructures critiques » le sont pour les infrastructures décrites à l'article 74b, à l'article 74b réduit du 74c, ou autrement ?

Article 76
Collaboration sur le plan national

Nous estimons qu'une collaboration avec le PFPDT s'avère indispensable au vu de l'obligation d'annonce à ses services prévus par la LPD.

Article 79, al 1, 1
[...] la durée de conservation est limitée à deux ans.

Nous proposons de préciser : [...] « après leur dernière utilisation ».

Chapitre II
2. Loi du 25 septembre 2020 sur la protection des données.

Article 24, al 5bis
Le PFPDT peut, avec l'accord du responsable tenu à l'obligation de signalement, transmettre le signalement au Centre national pour la cybersécurité à des fins d'analyse de l'incident.

Nous estimons que la collaboration doit être plus étroite, et qu'il convient de prévoir une communication contraignante de la part du NCSC au PFPDT ; la communication du PFPDT au bénéfice du NCSC n'a pas à obtenir l'autorisation de la personne responsable du signalement si ce dernier remplit les conditions de la présente loi.

Nous restons bien entendu à votre disposition pour tout complément d'information.